AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions of claims in the application:

1. (Canceled)

2. (Currently Amended) A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, said filtering including:

updating a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request; and

applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request ~~count~~ frequency;

and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

3. (Currently Amended) The method of claim 2, wherein said applying further comprises setting an alarm when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

4. (Original) The method of claim 3, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

5. (Currently Amended) The method of claim 2, wherein said applying further comprises dropping the data packet containing said request when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

6. (Currently Amended) The method of claim 2, wherein said applying further comprises shutting down the account used to access said first communication network when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

7. (Currently Amended) The method of claim 6, wherein said applying further comprises disabling HTTP requests for a hold-down period when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

8. (Currently Amended) The method of claim 7, further comprising increasing said hold-down period each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

9. (Currently Amended) The method of claim 8, wherein said hold-down period increases exponentially each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

10-12. (Canceled)

13. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to prevent denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, said filtering including:

updating a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request; and

applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request ~~count~~ frequency;

and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

14. (Currently Amended) The program storage device of claim 13, wherein said applying further comprises setting an alarm when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

15. (Original) The program storage device of claim 14, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

16. (Currently Amended) The program storage device of claim 13, wherein said applying further comprises dropping the data packet containing said request when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

17 (Currently Amended) The program storage device of claim 13, wherein said applying further comprises shutting down the account used to access said first communication network when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

18. (Currently Amended) The program storage device of claim 17, wherein said applying further comprises disabling HTTP requests for a hold-down period when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

19. (Currently Amended) The program storage device of claim 18, further comprising increasing said hold-down period each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

20. (Currently Amended) The program storage device of claim 19, wherein said hold-down period increases exponentially each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

21-23. (Canceled)

24. (Currently Amended) An apparatus for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the apparatus comprising:

means for receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

means for receiving a profile for said subscriber;

means for filtering to determine whether said subscriber is authorized to make said request based upon said profile, said means for filtering including:

means for updating a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request; and

means for applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request ~~count~~ frequency;

and

means for forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

25. (Currently Amended) The apparatus of claim 24, wherein said means for applying further comprises means for setting an alarm when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

26. (Original) The apparatus of claim 25, further comprising means for sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

27. (Currently Amended) The apparatus of claim 24, wherein said means for applying further comprises means for dropping the data packet containing said request when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

28. (Currently Amended) The apparatus of claim 24, wherein said means for applying further comprises means for shutting down the account used to access said first communication network when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

29. (Currently Amended) The apparatus of claim 28, wherein said means for applying further comprises means for disabling HTTP requests for a hold-down period

when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

30. (Currently Amended) The apparatus of claim 29, further comprising means for increasing said hold-down period each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

31. (Currently Amended) The apparatus of claim 30, wherein said hold-down period increases exponentially each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

32-35. (Canceled)

36. (Currently Amended) An apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, said apparatus comprising:

a first receiving interface capable of accepting a HTTP request received from a subscriber using a first communication network, said request including a Universal Resource Locator (URL);

a profile request generator capable of generating a profile request based upon said request;

a first forwarding interface capable of sending said profile request to an Authentication, Authorization, and Accounting (AAA) ~~AAA~~ server;

a second receiving interface capable of accepting a requested profile;

a filter capable of determining whether said request is authorized based upon said requested profile, said filter including:

an updater to update a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request; and

a responder to apply HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request ~~count~~ frequency;

an authorizer capable of allowing said request to be forwarded on at least one other communication network coupled to said first communication network; and

a second forwarding interface capable of forwarding said request on said at least one other communication network.

37. (Currently Amended) The apparatus of claim 36, wherein said responder further sets an alarm when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

38. (Currently Amended) The apparatus of ~~claim 36~~ claim 37, wherein said responder sends said alarm to an Internet Service Provider (ISP) associated with said subscriber.

39. (Currently Amended) The apparatus of claim 36, wherein said responder drops the data packet containing said request when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

40. (Currently Amended) The apparatus of claim 36, wherein said responder shuts down the account used to access said first communication network when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

41. (Currently Amended) The apparatus of claim 40, wherein said responder disables HTTP requests for a hold-down period when said client HTTP request ~~count~~ frequency exceeds said maximum HTTP request ~~count~~ frequency.

42. (Currently Amended) The apparatus of claim 41, wherein said responder increases said hold-down period each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

43. (Currently Amended) The apparatus of claim 42, wherein said responder increases said hold-down period exponentially each time said client HTTP ~~count~~ request frequency exceeds said maximum HTTP request ~~count~~ frequency.

44, 45. (Canceled)